UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,768	06/27/2003	Alexandru Gavrilescu	30835/305573	8097

45373 7590 10/31/2006

MARSHALL, GERSTEIN & BORUN LLP (MICROSOFT)
233 SOUTH WACKER DRIVE
6300 SEARS TOWER
CHICAGO, IL 60606

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/608,768	**Applicant(s)** GAVRILESCU ET AL.	
	Examiner Carlton Johnson	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 June 2003 and 08 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *6-3-2005*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed **6-27-2003**.

2. Claims **1 - 47** are pending. Claims **1, 20, 22, 26, 29, 32, 34, 36, 40, 43, 46** are independent.

Claim Objections - 35 USC § 112

3. Claim **15** cites the term *"friendly"* in the claim language. There is insufficient antecedent basis for this limitation within the claim or specification. The term can be defined as: *easy to understand or use.* It is unclear how this term is to be applied in this claim limitation. Appropriate correction is required.

4. Claims **25 and 39** cite the term *"back-off"* in the claim language. There is insufficient antecedent basis for this limitation within the claim or specification. The term can be defined as: *Relent, abandon one's stand.* It is unclear how this term is to be applied in this claim limitation. Appropriate correction is required.

5. Claims **31 and 45** cite the term *"deprecate"* in the claim language. There is insufficient antecedent basis for this limitation within the claim or specification. The term can be defined as: *" (1) To express disapproval of; deplore., and (2) To belittle;*

depreciate.". It is unclear how this term is to be applied in this claim limitation. Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of 35 U.S.C. 102(e) which forms the basis for all obviousness rejections set forth in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims **1 - 13, 18, 19, 26 - 31, 40 - 45** are rejected under 35 U.S.C. 102(e) as being anticipated by **Yeager et al.** (US PGPUB No. **20050086300**).

Regarding Claim 1, Yeager discloses a system for providing security to a graph of interconnected nodes, the system comprising:

a) a grouping multiplexing layer configured to monitor calls to the system; (see Yeager paragraph [0398], lines 1-16: monitor and response to call (i.e. requests) to system; *graph defined as collection of interconnected nodes- group defined as graph with provided security*)

b) a graphing dynamic link layer configured to transmit data to and from the graph; (see Yeager paragraph [0083], lines 3-9: link layer (i.e. network layer) for data transmissions; paragraph [0225], lines 9-13: pipes, communications channel for data transmission between peer; *graph defined as collection of interconnected nodes- group defined as graph with provided security*) and

c) a group security manager coupled to the grouping multiplexing layer and coupled to the graphing dynamic link layer, the group security manager configured to perform security-related acts via interacting with a group database to propagate security-related information to members of a group within the graph by controlling interactions between group members and a plurality of actions governing the group members. (see Yeager paragraph [0269], lines 1-12: security control on communications among group members; paragraph [0500], lines 1-13: multiple group actions performed; paragraph [0256], lines 1-3: storage, database utilized to contain content, peer, security information; *graph defined as collection of interconnected nodes- group defined as graph with provided security*)

Regarding Claim 2, Yeager discloses the system of claim 1 wherein the plurality of actions includes publishing of group records, validating records that for publication, discovering group members, enabling custom roles, enabling user-defined records, and enforcing security policies. (see Yeager paragraph [0402], lines 1-7: discover members; paragraph [0223], lines 6-11: publish content information or records; paragraph [0225], lines 4-9: mechanism, policies (i.e. protocol) for peer group and member discovery)

Regarding Claim 3, Yeager discloses the system of claim 1 wherein the group security manager generates events regarding certificates, roles and record types. (see Yeager paragraph [0135], lines 1-3; paragraph [0135], lines 5-11: certificate processing, role security information or records generated)

Regarding Claim 4, Yeager discloses the system of claim 1 wherein the group security manager provides security to data published according to a graphing protocol and enables secure connections to be established between peers in the graph. (see Yeager paragraph [0567], lines 1-12: secure communications, encryption (i.e. VPN) utilized)

Regarding Claim 5, Yeager discloses the system of claim 1 wherein the group security manager enables use of peer name resolution protocol to discover the group members. (see Yeager paragraph [0261], lines 5-8: name service; paragraph [0225], lines 4-9: mechanism, policies (i.e. protocol) for peer group and member discovery)

Regarding Claim 6, Yeager discloses the system of claim 1 wherein the group security manager enables peers in the graph with different capabilities to have different privileges with respect to other peers. (see Yeager paragraph [0134], lines 13-16: each peer, different set of privileges)

Regarding Claim 7, Yeager discloses the system of claim 1 wherein the group security manager requires each node in the group to have a secure peer name. (see Yeager paragraph [0261], lines 1-2; paragraph 269], lines 1-12: unique name for each peer, implementation secure boundaries between peer group (i.e. secure peer name))

Regarding Claim 8, Yeager discloses the system of claim 7 wherein the secure peer name is secured via being derived from a public key that is part of a public/private key pair. (see Yeager paragraph [0135], lines 3-5: public/private key pair cryptography utilized; Yeager paragraph [0269], lines 1-12: secure peer-to-peer processing environment, peer names encrypted (i.e. secured by usage of public key))

Regarding Claim 9, Yeager discloses the system of claim 1 wherein the group security manager requires each group to have a secure peer name based on a public/private key pair. (see Yeager paragraph [0135], lines 3-5: public/private key pair cryptography utilized; Yeager paragraph [0269], lines 1-12: secure processing within peer-to-peer environment, protect (i.e. secure) peer names)

Regarding Claim 10, Yeager discloses the system of claim 1 wherein the group security manager requires a plurality of membership credentials to participate in the group. (see Yeager paragraph [0313], lines 1-4; paragraph [0500], lines 1-13: credential(s) required for group membership)

Regarding Claim 11, Yeager discloses the system of claim 10 wherein the credentials are X.509 certificates. (see Yeager paragraph [0561], lines 4-7; paragraph [0593], lines 16-18: X.509 certificates utilized in authentication)

Regarding Claim 12, Yeager discloses the system of claim 10 wherein credentials define privileges for the group members, the privileges including different classes of group members. (see Yeager paragraph [0134], lines 10-16: different types of group members, each group has own security model and levels)

Regarding Claim 13, Yeager discloses the system of claim 10 wherein credentials have a validity period the credentials require renewal before they expire. (see Yeager paragraph [0591], lines 7-10: expiration time period for credentials)

Regarding Claim 18, Yeager discloses the system of claim 1 wherein the group security manager enables secure publishing to the group database by requiring data to be published to the group to contain a cryptographic signature. (see Yeager paragraph [00135], lines 1-3; paragraph [0135], lines 5-11: signature utilized for content, peer information or records)

Regarding Claim 19, Yeager discloses the system of claim 1 wherein the group security manager checks for authorization that a publisher has the right to publish each record and that a signer has the right to sign the record by checking privileges of the publisher and signer. (see Yeager paragraph [0223], lines 6-11: publish content, peer information; paragraph [00135], lines 1-3; paragraph [0135], lines 5-11: attach signature, signature utilized for content, peer information or record)

Regarding Claims 26, 40, Yeager discloses a method, computer-readable medium having computer-executable instructions to perform acts for ensuring that a publisher of information in a record to a secure group in a graph of interconnected nodes has authority to publish to the secure group, the method comprising:

a) creating a token (see Yeager paragraph [0577], lines 7-11: tokens, credentials utilized for security) for the publisher, the token containing information located in a role assigned to the publisher, the role identifying privileges of the publisher; (see Yeager paragraph [0578], lines 4-6: role assignments, privileges assigned) and

b) matching the token see Yeager paragraph [0577], lines 7-11: tokens, credentials utilized for security) against a security descriptor for the record to be published, the security descriptor providing a list of rights associated with each role. (see Yeager paragraph [0578], lines 4-6: privileges, access control list linked to role)

Regarding Claims 27, 41, Yeager discloses the method, computer-readable medium of claims 26, 40 wherein the token is published in a graph database, the graph database providing security related information to each member of the secure group. (see Yeager paragraph [0256], lines 1-3: storage, database containing security information)

Regarding Claims 28, 42, Yeager discloses the method, computer-readable medium of claims 27, 40 wherein the graph database enables deferred record validation by enabling a group member to defer until required security information is available to the group member. (see Yeager paragraph [0256], lines 1-3: storage, database containing peer information)

Regarding Claims 29, 43, Yeager discloses a method, computer-readable medium having computer-executable instructions to perform acts for revoking a member of a group of interconnected nodes within a graph, the method comprising:

a) publishing a revocation record to the group, the revocation record identifying the member; (see Yeager paragraph [0086], lines 1-6: software, computer readable medium; paragraph [0223], lines 6-11: publish content, peer information or records: publish content, peer information; paragraph [0558], lines 4-8: remove or revoke membership) and

b) revoking any records published by the member according to the revocation record. (see Yeager paragraph [0223], lines 6-11: publish content, peer information or records; paragraph [0558], lines 4-8: remove or revoke membership)

Regarding Claims 30, 44, Yeager discloses the method, computer-readable medium of claims 29, 43 wherein the revocation record is published with validation time sufficient to ensure that a current certificate of the revoked group member expires before the revocation. (see Yeager paragraph [0591], lines 7-10: expiration time period for credentials; paragraph [0558], lines 4-8: remove or revoke membership; paragraph [0135], lines 1-3; paragraph [0135], lines 5-11: certificate utilization)

Regarding Claims 31, 45, Yeager discloses the method, computer-readable medium of claim 29 wherein if the member to be revoked is an administrator, the administrator privileges are first deprecated prior to the publishing the revocation record. (see Yeager paragraph [0086], lines 1-6: software, computer readable medium; paragraph [0558], lines 4-8: some members, managers, administrators to remove membership in peer group)

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims **14 - 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yeager** in view of **Pabla et al.** (US Patent No. **20040162871**).

Regarding Claim 14, Yeager discloses the system of claim 12 where role defines the privileges for the group members. (see Yeager paragraph [0578], lines 4-6: role and access privileges are linked (i.e. defined)) Yeager does not specifically disclose a plurality of roles. However, Pabla discloses wherein a plurality of roles. (see Pabla paragraph [0312], lines 9-12: multiple roles)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Pabla to enable a plurality of roles. One of ordinary skill in the art would have been motivated to employ the teachings of Pabla in order to, within a cryptographic authentication environment, enable wireless devices to operate seamless as peer-to-peer devices within a network environment. (see Pabla paragraph [0019], lines 1-9: " ... *provide a mechanism for applications on wireless devices, such as MIDP devices, to participate as peers in peer-to-peer network environments ... desirable for this mechanism to be conservative in the usage of resources of the wireless devices, while still providing access to the peer-to-peer functionalities typically available to other peers in peer-to-peer network environments. ...* ")

Regarding Claim 15, Yeager discloses the system of claim 14 wherein a role is identified. (see Yeager paragraph [0578], lines 4-6: role designated) Yeager does not specifically disclose a name or a unique identifier for a role. However, Pabla discloses wherein each role is identified by a friendly name and a unique identifier. (see Pabla paragraph [0312], lines 12-17: unique identifier, name)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Pabla to enable a plurality of roles, and an identifier or name for each role. One of ordinary skill in the art would have been motivated to employ the teachings of Pabla in order to, within a cryptographic authentication environment, enable wireless devices to operate seamless as peer-to-peer devices within a network environment. (see Pabla paragraph [0019], lines 1-9)

Regarding Claim 16, Yeager discloses the system of claim 14 wherein the plurality of roles have a role hierarchy that governs abilities to publish, modify and delete records. (see Yeager paragraph [0578], lines 4-6: role capability; paragraph [0223], lines 6-11: publish, update content information or records) Yeager does not specifically disclose role hierarchy. However, Pabla discloses wherein the plurality of roles have a role hierarchy that governs abilities. (see Pabla paragraph [0312], lines 9-12: multiple roles; paragraph [0252], lines 1-4: role, hierarchical structure for services and applications, peers)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Pabla to enable a role hierarchy or a set of levels for roles. One of ordinary skill in the art would have been motivated to employ the teachings of Pabla in order to, within a cryptographic authentication environment, enable wireless devices to operate seamless as peer-to-peer devices within a network environment. (see Pabla paragraph [0019], lines 1-9)

Regarding Claim 17, Yeager discloses the system of claim 14 the plurality of roles can include a role authorizing group members to modify one or record and authorize the group members to grant themselves privileges to perform one or more operations in the group. (see Yeager paragraph [0578], lines 4-6: role, privileges within group; paragraph [0558], lines 4-8: update information; paragraph [0580], lines 2-6; paragraph [0580], lines 13-14: group access control, protocols, and policies setup by group members)

10. Claims **20 - 25, 34 - 39** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yeager** in view of **Yellepeddy et al.** (US Patent No. **20040111607**).

Regarding Claims 20, 34, Yeager discloses a method for a member in a group within a graph of interconnected peer nodes to granting privileges, the method comprising:

a) connecting to a second member in the group; (see Yeager paragraph [paragraph [0225], lines 9-13: pipes, communications channel for data transmission between peer members)

Yeager discloses wherein the capability to renew membership in a peer group, and wherein the renewal is based on authorization from the administrator or based on one or more security policies. (see Yeager paragraph [0558], lines 4-8: membership renewal (i.e. remove, add) capability; paragraph [0225], lines 4-9: security policies utilized) Yeager does not specifically disclose the capability to renew a certificate. However, Yellepeddy discloses:

b) requesting authorization from an administrator for renewing the certificate. (see Yellepeddy paragraph [0092], lines 1-5: renew certificate)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Yellepaddy to enable the capability to renew a certificate in the processing of authentication information. One of ordinary skill in the art would have been motivated to employ the teachings of Yellepaddy in order to, within a cryptographic authentication environment, optimize verification and validation of the availability of a certificate utilizing an online status check protocol. (see Yellepaddy paragraph [0010], lines 1-4: " ... *would be advantageous to have a method and system that for configuring a set of OCSP responders in order to improve the availability of each of the OCSP responders. ...* ")

Regarding Claims 21, 35, Yeager discloses the method, computer-readable medium of claims 20, 34 wherein the renewal is based on the security policies if the authorization from the administrator is not received. (see Yeager paragraph [0086], lines 1-7: software; paragraph [0225], lines 4-9: membership based on policies) Yeager does not specifically disclose the capability to renew a certificate. However, Yellepeddy discloses wherein the capability for the renewal of a certificate. (see Yellepeddy paragraph [0092], lines 1-5: renew certificate)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Yellepaddy to enable the capability to renew a certificate in the processing of authentication information. One of ordinary skill in the art would have been motivated to employ the teachings of Yellepaddy in order to, within a cryptographic authentication environment, to optimize verification and validation of the availability of a certificate utilizing an online status check protocol. (see Yellepaddy paragraph [0010], lines 1-4)

Regarding Claims 22,36, Yeager discloses a method, computer-readable medium having computer-executable instructions to perform acts for a member in a group within a graph of interconnected peer nodes to renew a certificate granting privileges, the method comprising:

Yeager discloses the capability to publish content, peer information or records (see Yeager paragraph [0086], lines 1-7: software, computer readable medium; paragraph [0223], lines 6-11: publish content, peer information or records), and the capability to renew membership based on security policies (see Yeager paragraph [0225], lines 4-9: renew membership). Yeager does not specifically disclose the capability to renew a certificate.

However, Yellepeddy discloses:

a) a request to renew the certificate; (see Yellepeddy paragraph [0011], lines 7-11: request; paragraph [0225], lines 4-9: renew certificate) and

b) performing renewal. (see Yellepeddy paragraph [0092], lines 1-5: renew certificate)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Yellepaddy to enable the capability to process a request to renew a certificate in the processing of authentication information. One of ordinary skill in the art would have been motivated to employ the teachings of Yellepaddy in order to, within a cryptographic authentication environment, to optimize verification and validation of the availability of a certificate utilizing an online status check protocol. (see Yellepaddy paragraph [0010], lines 1-4)

Regarding Claims 23, 37, Yeager discloses the method, computer-readable medium of claims 22, 36 wherein the renewal is performed online, the method further comprising:

the graph of interconnected nodes (see Yeager paragraph [0029], lines 1-6: multiple interconnected nodes). Yeager does not specifically disclose the capability to process a certificate chain, or renew a certificate.

However, Yellepeddy discloses:

a) contacting one or more authorized members with a shorter chain before contacting authorized members with a longer chain; (see Yellepeddy paragraph [0057], lines 16-19; paragraph [0079], lines 1-5; paragraph [0079], lines 14-22: certificate chain processing, chain length (i.e. short or long)) and

b) performing one or more renewal attempts to achieve a chain that is of shorter length, wherein number of renewal attempts are proportional to length of the chain; (see Yellepeddy paragraph [0057], lines 16-19; paragraph [0079], lines 1-5; paragraph [0079], lines 14-22: certificate chain processing, chain length (i.e. short or long); paragraph [0225], lines 4-9: renew certificate) and

c) if a chain is beyond a predetermined length, performing an offline renewal to shorten the chain. (see Yellepeddy paragraph [0057], lines 16-19; paragraph [0079], lines 1-5; paragraph [0079], lines 14-22: certificate chain processing, chain length (i.e. short or long); paragraph [0225], lines 4-9: renew certificate)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Yellepaddy to enable the capability to utilize a certificate chain, and renew a certificate in the processing of authentication information. One of ordinary skill in the art would have been motivated to employ the teachings of Yellepaddy in order to, within a cryptographic authentication environment, to optimize verification and validation of the availability of a certificate utilizing an online status check protocol. (see Yellepaddy paragraph [0010], lines 1-4)

Regarding Claims 24, 38, Yeager discloses the method, computer-readable medium of claims 22, 36. (see Yeager paragraph [0086], lines 1-7: software, computer readable medium) Yeager does not specifically disclose the capability to process a certificate chain, or renew a certificate. However, Yellepeddy disclose wherein the renewal is repeated if a shorter chain can be achieved. (see Yellepeddy paragraph [0057], lines 16-19; paragraph [0079], lines 1-5; paragraph [0079], lines 14-22: certificate chain processing, chain length (i.e. short or long); paragraph [0225], lines 4-9: renew certificate)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Yellepaddy to enable the capability to utilize a certificate chain, and renew a certificate in the processing of authentication information. One of ordinary skill in the art would have been motivated to employ the teachings of Yellepaddy in order to, within a cryptographic authentication environment, to optimize verification and validation of the availability of a certificate utilizing an online status check protocol. (see Yellepaddy paragraph [0010], lines 1-4)

Regarding Claims 25, 39, Yeager discloses the method, computer-readable medium of claims 22, 36 wherein more than one authorized member is the group is active, each authorized member in the group enabled to process the request. (see Yeager paragraph [0086], lines 1-7: software, computer readable medium; paragraph [0558], lines 4-8: more than one member authorized to process requests) Yeager does not specifically disclose the capability to process a certificate chain, or renew a certificate. However, Yellepeddy disclose wherein enabled to process the renewal request, providing each authorized member in the group with a random back-off prior to attempting to process the renewal request, the random back-off proportional to a length of the chain of the authorized member. (see Yellepeddy paragraph [0057], lines 16-19; paragraph [0079], lines 1-5; paragraph [0079], lines 14-22: certificate chain processing, chain length (i.e. short or long); paragraph [0092], lines 1-5: renewal of certificate)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Yellepaddy to enable the capability to utilize a certificate chain, and renew a certificate in the processing of authentication information. One of ordinary skill in the art would have been motivated to employ the teachings of Yellepaddy in order to, within a cryptographic authentication environment, to optimize verification and validation of the availability of a certificate utilizing an online status check protocol. (see Yellepaddy paragraph [0010], lines 1-4)

11. Claims **32. 33, 46, 47** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yeager** in view of **Aguilera et al.** (US Patent No. **20040243827**).

Regarding Claims 32, 46, Yeager discloses a method, computer-readable medium having computer-executable instructions to perform acts for revoking one or more members of a group of interconnected nodes within a graph, the method comprising:

a group of interconnected nodes or a graph (see Yeager paragraph [0029], lines 1-6: grouping of interconnected nodes), the usage of software for prior art implementation, and the usage of one or more serial numbers, the one or more serial numbers identifying the one or more members of the group. (see Yeager paragraph [0086], lines 1-7: software, computer-readable medium; paragraph [0173], lines 1-6: unique identification (i.e. UUID) or serial numbers as identification information) Yeager does not specifically disclose the usage or update of a revocation bitmap.

However, Aguilera discloses:

a) identifying one or more bits in a revocation bit map, the bits identifying the one or more members of the group; (see Aguilera paragraph [0031], lines 1-5: bitmap representation for revocation list) and

b) altering the one or more bits in the revocation bit map, the altering revoking the one or more members of the group. (see Aguilera paragraph [0031], lines 1-5: bitmap representation for revocation list; paragraph [0027], lines 17-20: update revocation list, in order to revoke an entity (i.e. member))

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Aguilera to enable a bitmap representation for revocation list information. One of ordinary skill in the art would have been motivated to employ the teachings of Aguilera in order to, within a cryptographic authentication peer-to-peer environment, enable the capability to utilize a small amount storage for the bitmap revocation information. (see Aquilera paragraph [0031], lines 1-5: " ... *It is worth noting that the group list and the revocation list can be stored as a bitmap or as explicit lists. The bitmap representation has the advantage that it is compact, but it requires capability identifiers to be small and thus limits the number of outstanding capabilities. ...* ")

Regarding Claims 33, 47, Yeager discloses the method, computer-readable medium of claims 32, 46. (see Yeager paragraph [0086], lines 1-7: software, computer-readable medium) Yeager does not specifically disclose the usage or update of a revocation bitmap. However, Aguilera discloses wherein the revocation bitmap is scalable. (see Aquilera paragraph [0031], lines 1-5: bitmap representation for revocation list; paragraph [0033], lines 1-3: scalable, adjustable size for bitmap representation)

It would have been obvious to one of ordinary skill in the art to modify Yeager as taught by Aguilera to enable a bitmap representation for revocation list information. One of ordinary skill in the art would have been motivated to employ the teachings of Aguilera in order to, within a cryptographic authentication peer-to-peer environment, enable the capability to utilize a small amount storage for the bitmap revocation information. (see Aquilera paragraph [0031], lines 1-5)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton Johnson whose telephone number is 571-270-1032. The examiner can normally be reached Monday through Friday from 8:00AM to 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar Moazzami, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

C.J.

Carlton Johnson
October 26, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/27/06